IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Nikhil JHINGAN, and Vinod Udharam VASNANI	§ § §	Confirmation No.:	3915
Serial No.:	09/808,553	§ § §	Group Art Unit:	2152
Filed:	March 14, 2001	§ § §	Examiner:	C. Zong
For:	A System And Method For Redirection Of User-Specific Data Storage Requests	§ § §	Attorney Docket No.:	2060-01400
			Client Docket No.:	SG516832US. FMK

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Date: July 21, 2006

Sir:

Appellant hereby submits this Appeal Brief in connection with the above-identified application. A Notice of Appeal was filed on March 28, 2006.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST 3
II. RELATED APPEALS AND INTERFERENCES 4
III. STATUS OF THE CLAIMS 5
IV. STATUS OF THE AMENDMENTS 6
V. SUMMARY OF THE CLAIMED SUBJECT MATTER 7
VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL 12
VII. ARGUMENT 13
A. Ussery 13
B. Kenner 14
C. Claims 21, 23, and 26-27 15
D. Claims 22 and 30 18
E. Claims 24 and 32 18
F. Claims 25 and 33 19
G. Claims 28 and 36 20
H. Claims 29, 31, and 34-35 20
VIII. CONCLUSION 24
IX. CLAIMS APPENDIX 25
X. EVIDENCE APPENDIX 29
XI. RELATED PROCEEDINGS APPENDIX 30

I. REAL PARTY IN INTEREST

The real party in interest is ACCELLION PTE LTD, which changed its name from SPACEDISK PTE LTD. The Change of Name document was recorded on September 24, 2001, at Reel/Frame 012194/0024. The original assignment from Nikhil Jhingan and Vinod Udharam to SPACEDISK PTE LTD was recorded on April 9, 2001, at Reel/Frame 011697/0252.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals or interferences.

III. STATUS OF THE CLAIMS

Originally filed claims:	1-20.	
Claim cancellations.	1-20.	
Added claims:		21-36.
Presently pending claims:	21-36.	
Presently appealed claims:	21-36.	

IV. STATUS OF THE AMENDMENTS

No amendments have been submitted after the final Office action dated November 28, 2005.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Embodiments of the invention provide methods and systems for storage, manipulation and distribution of user-specific content (USC) on the Internet. The term "user-specific content" refers to content created by one user to be accessed by the same user or by a few users (see Specification, page 3, lines 27-29).

The following provides a concise explanation of the subject matter defined in each of the claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable (*i.e.*, the claims are annotated using parenthesis). Note that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

21. (Previously presented) A method for storing and accessing user-specific data in a client-server computer network (see Figure 2 and page 10, lines 23-32), the method comprising the steps of:

a user performing, from a first computer (104), a login operation to a first server (106) in the network (see Figure 2 and page 10, lines 23-32);

determining, based on the login operation performed by the user and a location of the first computer (104) in the network, a second server (202) in the network for storing user-specific data (see Figure 5 and page 12, line 8 – page, line 2);

the user sending, from the first computer (104) to the first server (106) in the network, a request to store the user-specific data (see Figure 5 and page 12, line 8 – page 13, line 10);

redirecting the request to the second server (202) for storing of the user-specific data at the second server (202) (see Figure 5 and page 12, line 8 – page 13, line 10); and

conducting a data upload directly between the first computer (104) and the second server (202) to store the user-specific data at the second server (202) (see Figure 5 and page 12, line 8 – page 13, line 10).

22. (Previously presented) The method as claimed in claim 21, wherein the first server (106) comprises an application server element (App Server, Figure 5) and a determination server element (iDNS, Figure 5) and the method comprises the user performing the login operation to the application server element, and the application server element performing another login operation to the determination server element based on the login operation performed by the user, for determining, based on the location of the first computer (104) in the network, the second server (202) in the network for storing the user-specific data (see Figure 6 and page 13, lines 22-28).

23. (Previously presented) The method as claimed in claim 22, wherein the application server element (App Server, Figure 5) and the determination server element (iDNS, Figure 5) are located on different computers in the network (see page 12, lines 4-6).

24. (Previously presented) The method as claimed in claim 21, further comprising the user or another user performing a login operation to the first server (106) from a second computer (104) and sending a request relating to said user-specific data to the first server (106); redirecting the request to the second server (202) based on the login operation from the second computer (104); and conducting transactions relating to the user-specific data directly between the second computer (104) and the second server (202) (see Figure 4).

25. (Previously presented) The method as claimed in claim 24, further comprising the steps of replicating at least a portion of the user-specific data on a third server (202B) selected based on a location of the second computer

(104) on the network, and redirecting requests relating to the user-specific data from the second computer (104) to the third server (202B) (see Figure 8 and page 16, line 13 – page 17, line 5).

26. (Previously presented) The method as claimed in claim 21, wherein the step of determining, based on a location of the first computer (104) in the network, the second server (202) in the network for storing the user-specific data comprises measuring respective response times between the first computer (104) and each of a plurality of candidate servers (see Figure 4-5 and page 12, line 20 – page 13, line 3).

27. (Previously presented) The method as claimed in claim 26, wherein the candidate server having the shortest response time is determined as the second server (202) (see Figure 4-5 and page 12, line 20 – page 13, line 3).

28. (Previously presented) The method as claimed in claim 21, wherein transactions between the first computer (104) and the second server (202) are conducted in an encrypted manner (see page 13, lines 26-28).

29. (Previously presented) A system for storing and accessing user-specific data in a client-server computer network (102, Figure 1), the system comprising:

a first server (106);

a first computer (104) operated by a user for performing a login operation to the first server (106) and for sending a request to store user-specific data to the first server (106) (see Figure 2 and page 10, lines 23-32);

wherein the first server (106) determines, based on the login operation performed by the user and a location of the first computer (104) in the network, a second server (202) for storing the user-specific data and redirects the request to the second server (202) for storing of the user-specific data at the second server (202) (see Figure 5 and page 12, line 8 – page 13, line 10),

wherein a data upload to store the user-specific data at the second server (202) is conducted directly between the first computer (104) and the second server (202) (see Figure 5 and page 12, line 8 – page 13, line 10).

30. (Previously presented) The system as claimed in claim 29, wherein the first server (106) comprises an application server element (App Server, Figure 5), and

a determination server element (iDNS, Figure 5),

wherein the application server element receives the login operation by the user and performs another login operation to the determination server element based on the login operation performed by the user for determining, based on the location of the first computer (104) in the network, the second server (202) in the network for storing the user-specific data (see Figure 6 and page 13, lines 22-28).

31. (Previously presented) The system as claimed in claim 30, wherein the application server element (App Server, Figure 5) and the determination server element (iDNS, Figure 5) are located on different computers in the network (see page 12, lines 4-6).

32. (Previously presented) The system as claimed in claim 29, further comprising a second computer (104) operated by the user or another user for performing a login operation to the first server (106) and for sending a request relating to the user-specific data to the first server (106); wherein the first server (106) redirects the request to the second server (202) based on the login operation from the second computer (104) and wherein transmissions relating to the user-specific data are conducted directly between the second computer (104) and the second server (202) (see Figure 4).

33. (Previously presented) The system as claimed in claim 32, wherein the first server (106) facilitates replication of at least a portion of the user-specific

data on a third server (202B) selected based on a location of the second computer (104) on the network, and redirects requests relating to the user-specific content from the second computer (104) to the third server (202B) (see Figure 8 and page 16, line 13 – page 17, line 5).

34. (Previously presented) The system as claimed in claim 29, wherein the first server (106) measures respective response times between the first computer (102) and each of a plurality of candidate servers during determining the second server (202) for storing the user-specific data (see Figure 4-5 and page 12, line 20 – page 13, line 3).

35. (Previously presented) The system as claimed in claim 34, wherein the first server (106) determines the candidate server having the shortest response time as the second server (202) (see Figure 4-5 and page 12, line 20 – page 13, line 3).

36. (Previously presented) The system as claimed in claim 29, wherein the system is arranged such that transactions between the first computer (104) and the second server (202) are conducted in an encrypted manner (see page 13, lines 26-28).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 21, 23 and 26-27 are unpatentable over U.S. Patent Publication No. 2002/0049903 ("Ussery") in view of U.S. Patent No. 6,112,239 ("Kenner")

Whether claims 22 and 30 are unpatentable over Ussery in view of Kenner

Whether claims 24 and 32 are unpatentable over Ussery in view of Kenner

Whether claims 25 and 33 are unpatentable over Ussery in view of Kenner

Whether claims 28 and 36 are unpatentable over Ussery in view of Kenner

Whether claims 29, 31, and 34-35 are unpatentable over Ussery in view of Kenner

VII. ARGUMENT

The Examiner erred in rejecting claims 21-36 as being unpatentable over U.S. Patent Publication No. 2002/0049903 ("Ussery") in view of U.S. Patent No. 6,112,239 ("Kenner"). The references cited by the Examiner are summarized below.

A. Ussery

Ussery teaches a system that repeatedly divides a database into portions and stores the portions in distributed memory units. The portions can be reassembled in response to a security clearance. Ussery's Figure 2 illustrates the system. In describing Figure 2, Ussery states "[a]ccess controller 104 operates, in any scenario, to repeatedly establish views of one of the selectable records in response to security controller 106 redistributing portions 101a-101n of the database 101 over distributed memory units 108-112" (paragraph [0051]). Also, "a user at terminal 204 accesses Intranet server 202 which identifies the user and passes the request to database server 100. A security clearance is entered and user 204 is passed to database administrator 102 and access controller 104. The user then enters a login that is based on a previously created profile table and, if the login is correct, then the request for a view of data records is passed to security controller 106. Security controller 106 then assembles the appropriate data records from database portions 101a-101n from

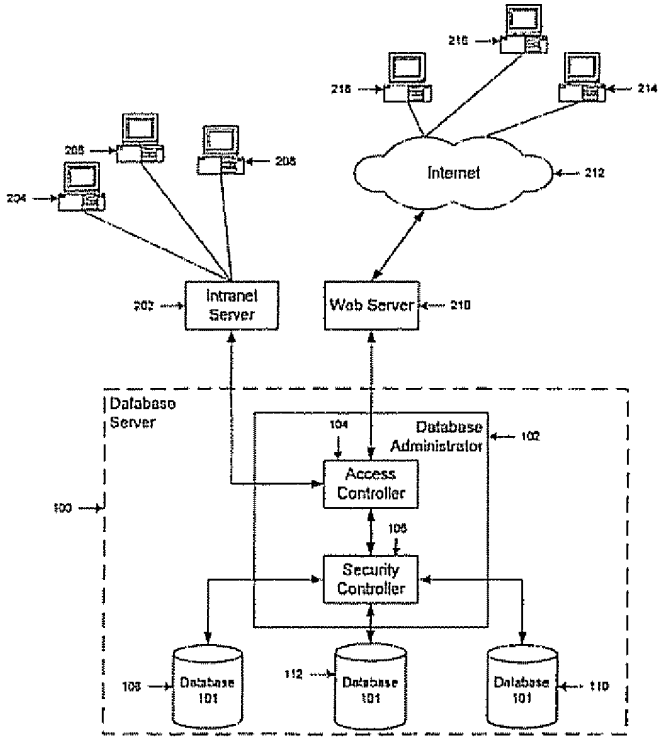


FIGURE 2

distributed memory units 108-112" (paragraph [0053]). By dividing data records and only reassembling upon proper security clearance, an unauthorized user is unable to view all the data records together.

B. Kenner

Kenner teaches a "smart" mirroring system for delivering video data. Kenner's Figure 1 illustrates the system. In describing Figure 1, Kenner states "[t]he configuration utility 34, when first run on the user terminal 12, retrieves a delivery site file from the MSP 32.... This delivery site file contains a list of all available delivery sites (such as delivery sites 26, 28, and 30) and a list of network tests to be run at the user terminal 12" (col. 8, lines 43-51). Also, "[a]fter all specified testes are run, the results are collected and processed" (col. 11, lines 61-62). Also, the configuration utility 34 relies primarily on ping and throughput tests for each available delivery site" (col., 12, lines 50-52). Also, "on the basis of the collected test results, and on information provided in the delivery site file by the MSP 32, the configuration utility 34 determines which delivery site, or group of delivery sites, is best for the user terminal 12" (col. 12, lines 41-45). Importantly, the configuration utility 34 determines where to download data from, but does not determine where to upload data to.

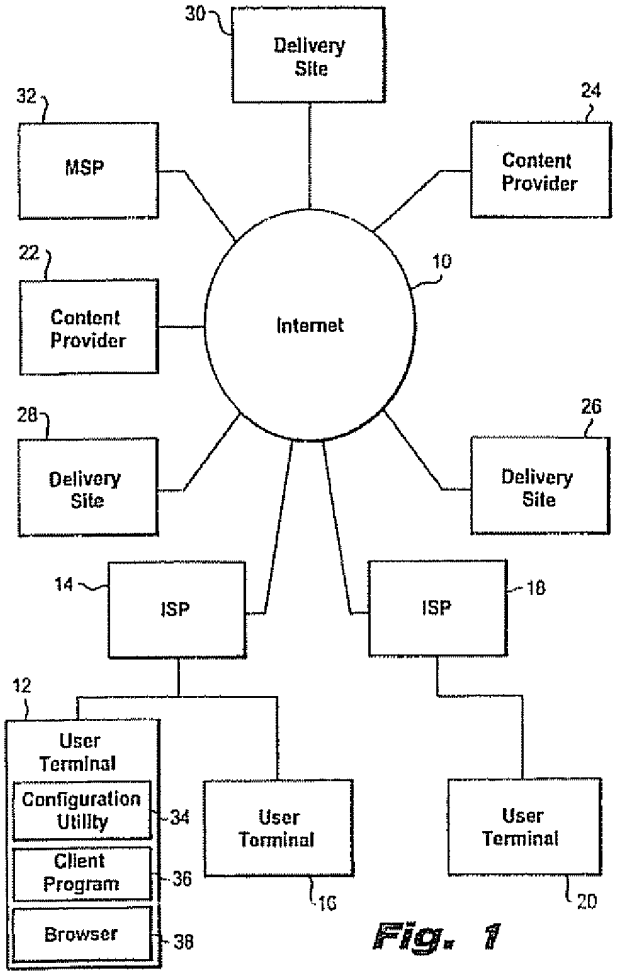


Fig. 1

C. Claims 21, 23, and 26-27

The Examiner improperly rejected claim 21 for at least the following reasons. First, claim 21 requires "a user performing, from a first computer, a login operation to a first server in the network" and "determining, based on the login operation performed by the user and a location of the first computer in the network, a second server in the network for storing user-specific data". In rejecting claim 21, the Examiner construes the second server as Ussery's database server 100 (Figure 2), and the first server as Ussery's intranet server 202. However, Ussery clearly discloses that "... user 204 is passed to database administrator 102 and access controller 104. The user then enters a login that is based on a previously created profile table and, if the login is correct, then the request for a view of data record is passed to security controller 106" (see paragraph [0053]). Ussery also states "when an authorized user logs into database server 100, ..." (see paragraph [0046]). Therefore, Ussery does not disclose a login operation to the first server as claimed in claim 21, but to the second server itself.

Second, Ussery is concerned with security of client data, as opposed to any relationship between the location of the first computer in the network, and a server to store data. In Ussery, the division of database 101 serves to achieve security in terms of unavailability of the "complete" data in anyone of the databases 101. Appellants refer to paragraphs [0129] to [0131] of Ussery, which, in explaining the principles of the disclosure, emphasize the security aspect of data in the divided database 101a-101n, and is completely silent on any association of the location of the client terminals (items 204, 206, and 208 in Ussery, Figure 2) and the selection of the second server as claimed in claim 21.

Appellants further refer to paragraph [0054] of Ussery which describes the operation of security controller 106 to repeatedly divide database 101 and to store portions to ones of distributed memory units 108 to 112. Importantly, again, there is no disclosure or suggestion whatsoever of selecting a second server based on the login operation performed by the user and a location of the first computer in the network, as set forth in claim 21.

The Examiner argues that the disclosure in Ussery may be combined with the disclosure in Kenner to arrive at the aforementioned feature. However, with reference to our submissions above, we respectfully submit that there would be no motivation whatsoever for a person of ordinary skill to consider a modification of the disclosure in Ussery to arrive at the aforementioned feature of claim 21. As is well established, the motivation of combining prior art documents must come from the prior art itself, and not from a reading of the present specification.

Furthermore, Appellants respectfully submit that Kenner does not disclose selecting a second server based on the login operation performed by the user and a location of the first computer in the network for conducting a data upload between the first computer and the second server to store user-specific data at the second server, as claimed in claim 21. Rather, as admitted by the Examiner, Kenner only discloses a "smart mirroring" system for distribution of mirror sites to direct user requests for web content. As is evident from the entire description in Kenner, for example at column 5, lines 7 to 19, or column 8, lines 7 to 19, or column 21, lines 36 to 51, Kenner is only concerned with delivery or downloading of content, such as video clips, as opposed to any consideration of data upload as set forth in claim 21.

Appellants respectfully submit that the abovementioned feature of claim 21 is clearly distinguished from a simple "reversal" of the systems disclosed in Kenner. In particular, uploading data and downloading data rely on two different requests in a client-server computer network, namely a "GET" request is used to download data as in Kenner, and a "POST" request is used to upload data as in the present invention.

The GET download request for data such as the delivery of an image or file in Kenner can be easily redirected. The redirection occurs by sending a response back to the client's browser from a first server, the response alerting the client's browser to go to another server to get the data. This alerting is caused by the presence of a redirect request incorporated into the "header" of the returned GET request by the first server. That modified GET request is the response to the client server.

In contrast, a request to upload a file, such as in a HTTP POST request, includes the entire content of the file along with the call for action to store the file. Thus, if an alleged "simple reversal" of Kenner was applied for an upload scenario, the first server receiving the HTTP POST request would return the HTTP POST request (including the entire content of the file) to the first computer while alerting the client/user to send the request to another server effected by the presence of a redirect request incorporated into the "header" of the returned HTTP POST request by the first server. Accordingly, the entire content would be "moved" in each communication between the server(s) and the first computer. Clearly, this would be an unworkable/undesirable solution.

In contrast to this alleged "simple reversal" solution suggested by the Examiner, the present invention as defined in claim 21 determines, based on a login operation performed by the user and a location of the computer from which the login operation is performed, a second server in the network for storing user-specific data. Upon a request to store user-specific data, the request is redirected to the second server for storing of the user-specific data at the second server. In other words, a POST request can immediately contain the destination information because of the above-mentioned determination step on login of the present invention. Therefore, the present invention provides an inventive solution, in which content does not have to be moved unnecessarily between the server(s) and the browser. Furthermore, there is no incentive or motivation found in Kenner to modify the disclosure in Kenner so as to arrive at the aforementioned feature of claim 21. Therefore, even if Kenner could be combined with Ussery, which we respectfully submit it cannot for the reasons outlined above, a person of ordinary skill would still not arrive at the aforementioned feature without performing a further inventive step. Based on the foregoing, Appellants respectfully submit that claim 21 is not obvious in light of Ussery and Kenner and the rejection of this grouping should be reversed.

D. Claims 22 and 30

In addition to the reasons provided with respect to claim 21, the rejection of claim 22 should be reversed for at least the following reasons. Claim 22 requires "the first server comprises an application server element and a determination server element and the method comprises the user performing the login operation to the application server element, and the application server element performing another login operation to the determination server element based on the login operation performed by the user, for determining, based on the location of the first computer in the network, the second server in the network for storing the user-specific data."

Appellants respectfully submit that there is no disclosure in Ussery of at least another login operation between an application server element and a determination server element based on the login operation performed by the user, for determining, based on the location of the first computer in the network, the second server in the network for storing the user-specific data. In Ussery, the access controller 104 passes a request for a view of data records to security controller 106 (see paragraph [0053]). There is no disclosure or suggestion of any further login operation between the access controller 104 and the security controller 106. Furthermore, with reference to paragraph [0054], Ussery fails to teach any further login operation based on the login operation performed by the user between the security controller 106 and any other downstream elements such as database portions 101a-101n. Based on the foregoing, Appellants respectfully submit that claim 22 is not obvious in light of Ussery and Kenner and the rejection of this grouping should be reversed

E. Claims 24 and 32

In addition to the reasons provided with respect to claim 21, the rejection of claim 24 should be reversed for at least the following reasons. Claim 24 requires "the user or another user performing a login operation to the first server from a second computer and sending a request relating to said user-specific data to the first server, redirecting the request to the second server based on the login

operation from the second computer, and conducting transactions relating to the user-specific data directly between the second computer and the second server."

Ussery fails to distinguish between the user or another user performing a login operation to the first server from two different computers but relating to the same user-specific data. The invention as defined in claim 24 provides that subsequent requests relating to the initially created user-specific data will be redirected based on the login operation from the second computer (*i.e.*, the one determined previously based on the location of the first computer from which the data was initially uploaded), as opposed to determining a suitable second server based on the location of the second computer. The invention defined in claim 24 is particularly useful for example where a user wishes to access his data while traveling (*i.e.*, from a temporary location), for which the user would not desire a "transfer" of his data to a server based on the location of another, temporary, computer used for the data access during his travels. Based on the foregoing, Appellants respectfully submit that claim 24 is not obvious in light of Ussery and Kenner and the rejection of this grouping should be reversed.

F. Claims 25 and 33

In addition to the reasons provided with respect to claims 21 and 24, the rejection of claim 25 should be reversed for at least the following reasons. Claim 25 requires "replicating at least a portion of the user-specific data on a third server selected based on a location of the second computer on the network, and redirecting requests relating to the user-specific data from the second computer to the third server."

Ussery does not link location of any of the user terminals (204, 206, 208, Figure 2) to selection of any servers. Furthermore, any disclosure of "moving" data by the security controller 106 between the different database portions 101a-101n does not serve a replication purpose. Rather, in stark contrast, the purpose in Ussery is division of data into portions, and distribution of portions among different locations for security purposes. Replication of data would be seen as compromising the entire purpose of the disclosure in Ussery.

The invention defined in claim 25 is useful, for example, where a user intends to repeatedly access his data from a temporary location, in which case replication of at least a portion of the data on a third server selected based on the location of the second computer can be desirable, for example for consideration of access speed. Based on the foregoing, Appellants respectfully submit that claim 25 is not obvious in light of Ussery and Kenner and the rejection of this grouping should be reversed.

G. Claims 28 and 36

In addition to the reasons provided with respect to claim 21, the rejection of claim 28 should be reversed for at least the following reasons. Claim 28 requires that "transactions between the first computer and the second server are conducted in an encrypted manner."

The Examiner improperly suggests that Ussery teaches encryption at paragraphs [0046], [0048] and [0053]. These paragraphs simply mention a login process and security clearance without mentioning data encryption. Based on the foregoing, Appellants respectfully submit that claim 28 is not obvious in light of Ussery and Kenner and the rejection of this grouping should be reversed.

H. Claims 29, 31, and 34-35

The Examiner improperly rejected claim 29 for at least the following reasons. First, claim 29 requires "a first computer operated by a user for performing a login operation to the first server and for sending a request to store user-specific data to the first server". Claim 29 further requires that "the first server determines, based on the login operation performed by the user and a location of the first computer in the network, a second server for storing the user-specific data and redirect the request to the second server for storing of the user-specific data at the second server". In rejecting claim 29, the Examiner construes the second server as Ussery's database server 100 (Figure 2), and the first server as Ussery's intranet server 202. However, Ussery clearly discloses that "... user 204 is passed to database administrator 102 and access controller 104. The user then enters a login that is based on a previously created profile table and, if the login is correct, then the request for a view of data record is passed to

security controller 106" (see paragraph [0053]). Ussery also states "when an authorized user logs into database server 100, ..." (see paragraph [0046]). Therefore, Ussery does not disclose a login operation to the first server as claimed in claim 29, but to the second server itself.

Second, Ussery is concerned with security of client data, as opposed to any relationship between the location of the first computer in the network, and a server to store data. In Ussery, the division of database 101 serves to achieve security in terms of unavailability of the "complete" data in anyone of the databases 101. Appellants refer to paragraphs [0129] to [0131] of Ussery, which, in explaining the principles of the disclosure, emphasize the security aspect of data in the divided database 101a-101n, and is completely silent on any association of the location of the client terminals (items 204, 206, and 208 in Ussery, Figure 2) and the selection of the second server as set forth in claim 29.

Appellants further refer to paragraph [0054] of Ussery which describes the operation of security controller 106 to repeatedly divide database 101 and to store portions to ones of distributed memory units 108 to 112. Importantly, again, there is no disclosure or suggestion whatsoever of selecting a second server based on the login operation performed by the user and a location of the first computer in the network, as set forth in claim 29.

The Examiner argues that the disclosure in Ussery may be combined with the disclosure in Kenner to arrive at the aforementioned feature. However, with reference to our submissions above, we respectfully submit that there would be no motivation whatsoever for a person of ordinary skill to consider a modification of the disclosure in Ussery to arrive at the aforementioned feature of claim 29. As is well established, the motivation of combining prior art documents must come from the prior art itself, and not from a reading of the present specification.

Furthermore, Appellants respectfully submit that Kenner does not disclose "a data upload to store the user-specific data at the second server is conducted directly between the first computer and the second server" as set forth in claim 29. Rather, as admitted by the Examiner, Kenner only discloses a "smart mirroring" system for distribution of mirror sites to direct user requests for web

content. As is evident from the entire description in Kenner, for example at column 5, lines 7 to 19, or column 8, lines 7 to 19, or column 21, lines 36 to 51, Kenner is only concerned with delivery or downloading of content, such as video clips, as opposed to any consideration of data upload as set forth in claim 29.

Appellants respectfully submit that the abovementioned feature of claim 29 is clearly distinguished from a simple "reversal" of the systems disclosed in Kenner. As previously explained with respect to claim 21, a "GET" request for downloading data as in Kenner is not the same as a "POST" request as in the present invention.

Again, the GET download request for data such as the delivery of an image or file in Kenner can be easily redirected. In contrast, a request to upload a file, such as in a HTTP POST request, includes the entire content of the file along with the call for action to store the file. Thus, if an alleged "simple reversal" of Kenner was applied for an upload scenario, the first server receiving the HTTP POST request would return the HTTP POST request (including the entire content of the file) to the first computer while alerting the client/user to send the request to another server effected by the presence of a redirect request incorporated into the "header" of the returned HTTP POST request by the first server. Accordingly, the entire content would be "moved" in each communication between the server(s) and the first computer. Clearly, this would be an unworkable/undesirable solution.

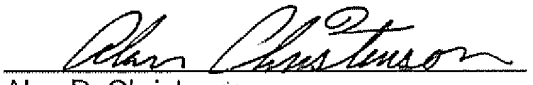
In contrast to this alleged "simple reversal" solution suggested by the Examiner, the first server as defined in claim 29 determines, based on the login operation performed by the user and a location of the first computer, a second server for storing of the user-specific data. Upon a request to store user-specific data, the request is redirected to the second server for storing of the user-specific data at the second server. In other words, a POST request can immediately contain the destination information based on the login operation of the present invention. Therefore, the present invention provides an inventive solution, in which content does not have to be moved unnecessarily between the server(s) and the browser. Furthermore, there is no incentive or motivation found in

Kenner to modify the disclosure in Kenner so as to arrive at the aforementioned feature of claim 29. Therefore, even if Kenner could be combined with Ussery, which we respectfully submit it cannot for the reasons outlined above, a person of ordinary skill would still not arrive at the aforementioned feature without performing a further inventive step. Based on the foregoing, Appellants respectfully submit that claim 29 is not obvious in light of Ussery and Kenner and the rejection of this grouping should be reversed.

VIII. CONCLUSION

For the reasons stated above, Appellants respectfully submit that the Examiner erred in rejecting all pending claims. It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. If any fees or time extensions are inadvertently omitted or if any fees have been overpaid, please appropriately charge or credit those fees to Conley Rose Deposit Account Number 03-2769 and enter any time extension(s) necessary to prevent this case from being abandoned

Respectfully submitted,



Alan D. Christenson
PTO Reg. No. 54,036
CONLEY ROSE, P.C.
(713) 238-8000 (Phone)
(713) 238-8008 (Fax)
AGENT FOR APPELLANTS

IX. CLAIMS APPENDIX

1-20. Cancelled.

21. (Previously presented) A method for storing and accessing user-specific data in a client-server computer network, the method comprising the steps of:

a user performing, from a first computer, a login operation to a first server in the network;

determining, based on the login operation performed by the user and a location of the first computer in the network, a second server in the network for storing user-specific data;

the user sending, from the first computer to the first server in the network, a request to store the user-specific data;

redirecting the request to the second server for storing of the user-specific data at the second server; and

conducting a data upload directly between the first computer and the second server to store the user-specific data at the second server.

22. (Previously presented) The method as claimed in claim 21, wherein the first server comprises an application server element and a determination server element and the method comprises the user performing the login operation to the application server element, and the application server element performing another login operation to the determination server element based on the login operation performed by the user, for determining, based on the location of the first computer in the network, the second server in the network for storing the user-specific data.

23. (Previously presented) The method as claimed in claim 22, wherein the application server element and the determination server element are located on different computers in the network.

24. (Previously presented) The method as claimed in claim 21, further comprising the user or another user performing a login operation to the first server from a second computer and sending a request relating to said user-specific data to the first server; redirecting the request to the second server based on the login operation from the second computer; and conducting transactions relating to the user-specific data directly between the second computer and the second server.

25. (Previously presented) The method as claimed in claim 24, further comprising the steps of replicating at least a portion of the user-specific data on a third server selected based on a location of the second computer on the network, and redirecting requests relating to the user-specific data from the second computer to the third server.

26. (Previously presented) The method as claimed in claim 21, wherein the step of determining, based on a location of the first computer in the network, the second server in the network for storing the user-specific data comprises measuring respective response times between the first computer and each of a plurality of candidate servers.

27. (Previously presented) The method as claimed in claim 26, wherein the candidate server having the shortest response time is determined as the second server.

28. (Previously presented) The method as claimed in claim 21, wherein transactions between the first computer and the second server are conducted in an encrypted manner.

29. (Previously presented) A system for storing and accessing user-specific data in a client-server computer network, the system comprising:

a first server;

a first computer operated by a user for performing a login operation to the first server and for sending a request to store user-specific data to the first server;

wherein the first server determines, based on the login operation performed by the user and a location of the first computer in the network, a second server for storing the user-specific data and redirects the request to the second server for storing of the user-specific data at the second server,

wherein a data upload to store the user-specific data at the second server is conducted directly between the first computer and the second server.

30. (Previously presented) The system as claimed in claim 29, wherein the first server comprises an application server element, and

a determination server element,

wherein the application server element receives the login operation by the user and performs another login operation to the determination server element based on the login operation performed by the user for determining, based on the location of the first computer in the network, the second server in the network for storing the user-specific data.

31. (Previously presented) The system as claimed in claim 30, wherein the application server element and the determination server element are located on different computers in the network.

32. (Previously presented) The system as claimed in claim 29, further comprising a second computer operated by the user or another user for performing a login operation to the first server and for sending a request relating to the user-specific data to the first server; wherein the first server redirects the request to the second server based on the login operation from the second computer and wherein transmissions relating to the user-specific

data are conducted directly between the second computer and the second server.

33. (Previously presented) The system as claimed in claim 32, wherein the first server facilitates replication of at least a portion of the user-specific data on a third server selected based on a location of the second computer on the network, and redirects requests relating to the user-specific content from the second computer to the third server.

34. (Previously presented) The system as claimed in claim 29, wherein the first server measures respective response times between the first computer and each of a plurality of candidate servers during determining the second server for storing the user-specific data

35. (Previously presented) The system as claimed in claim 34, wherein the first server determines the candidate server having the shortest response time as the second server.

36. (Previously presented) The system as claimed in claim 29, wherein the system is arranged such that transactions between the first computer and the second server are conducted in an encrypted manner.

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.